覗き見攻撃耐性を考慮した スマートフォンにおけるリズム認証手法
-楽曲の主旋律を用いた際の認証精度評価-

市村亮太[†1]　納富一宏[†1]　斎藤恵一[†2]

本研究では，スマートフォンにおける覗き見攻撃耐性を考慮したうえで，安全性，利便性を兼ねた認証手法について提案を行っている．先行研究では，覗き見攻撃耐性を考慮した入力方法として，画面を見ている状態で入力を行う「通常入力」に，本手法ならではの入力方法，画面を見ていない状態で入力を行う「覗き見防止入力」を提案し，実用可能であることを示した．次に，音楽経験年数で 2 つのグループに分け，認証精度に差が生じるか検証実験を行った．結果，認証精度には 4.0%の差ができた．音楽経験年数により認証精度に差が生じることは，利用者を限定してしまうことに繋がるため，この差をなくす必要がある．そこで本稿では，指定した楽曲の主旋律を用いリズムを作成した際に，先行研究に比べ認証精度が向上するかを検証するためのリズム認証実験を行った．指定楽曲(long)と指定楽曲(short)の 2 パターン計測し，特徴を自己組織化マップにより学習・分類し，分析を行った結果について述べる．指定楽曲(long)では認証精度 96.2%，指定楽曲(short)では認証精度 98.3%が得られ，どちらも先行研究に比べ認証精度は向上した．

A Rhythm Authentication Method Against Shoulder-Surfing Attack for Smartphone
- An Authentication Accuracy Evaluation using Melody of Musical Piece -

RYOTA ICHIMURA[†1]　KAZUHIRO NOTOMI[†1]　KEIICHI SAITO[†2]

1. はじめに

近年，スマートフォンなどのタッチスクリーンデバイスが普及してきている．これらは，入力デバイスと表示デバイスが一体化しており，第三者による覗き見攻撃によって入力情報を読み取られやすいことがいえる [1]．覗き見攻撃は，利用者の端末操作の様子を覗き見て，重要情報を盗み出す手口のことである．被害の代表例としては，銀行 ATM 操作時における背後からの覗き見による暗証番号の盗難が挙げられる．

こうした問題点から，本研究では，スマートフォンにおけるリズム認証の提案を行っている．リズム認証は，バイオメトリクス認証の一種である．バイオメトリクスとリズム認証については，2 章で述べる．

先行研究では，覗き見攻撃耐性を考慮した入力方法として，画面を見ている状態で入力を行う「通常入力」に，本手法ならではの入力方法として，画面を見ていない状態で入力を行う「覗き見防止入力」を提案し，認証精度に差が生じるか検証を行った．結果，認証精度は「通常入力」において 94.4%,「覗き見防止入力」において 93.6%となった．認証精度は同程度であり，「覗き見防止入力」が実用可能であることがわかっている [2]．また，音楽経験年数により認証精度に差が生じることは，利用者を限定してしまうことに繋がるため，検証を行う必要があると考えた．そこで，音楽経験年数 6 年以上と 3 年以下で 2 つのグループに分け，検証実験を行った．結果，音楽経験年数 6 年以上のグループ 1 は認証精度 98.9%，3 年以下のグループ 2 では認証精度 94.9%となった．認証精度は 4.0%の差ができ，この差をなくす必要がある [3]．

リズム認証は，リズムを作成し，登録を行い，認証を実行するという流れになっている．先行研究の手法は，リズムを作成する際,利用者自身がリズムを一から考えている．しかしこれでは，リズムが単調なものに偏る可能性があることや，時間の経過により，リズムを再現することが困難になるなどの問題点がある．

そこで本稿では，スマートフォンを用いたリズム認証手法において，指定した楽曲の主旋律を用いリズムを作成した際に，先行研究に比べ認証精度が向上するかを検証するためのリズム認証実験を行う．分析には，ニューラルネットワークの一種である自己組織化マップ（SOM：Self-Organizing-Maps，以下 SOM ）[4]を用い，その結果について考察する．

†1 神奈川工科大学大学院工学研究科情報工学専攻
Dept. of Information and Computer Sciences, Kanagawa Institute of Technology
†2 国際医療福祉大学情報教育室
Education Center of Medical Informatics, International University of Health and Welfare

2. バイオメトリクスとリズム認証

バイオメトリクスの技術的な定義は「行動的あるいは身体的な特徴を用い，個人を自動的に同定する技術」である[5]．バイオメトリクスは普遍性，唯一性，永続性の 3 つの性質をもっており，身体的特徴と行動的特徴の 2 種類がある．前者は，指紋，掌形，顔，虹彩などが相当し，後者は，声紋，署名，キーストロークが相当する．これらは随意的な要素があるために，上記の身体計測的なバイオメトリクスと異なり行動的特徴と呼ばれる．

リズム認証とは，バイオメトリクスの行動的特徴に該当する認証である[6]．タッチスクリーンのキャンバス上をタップする際のパターン，リズムにより個人識別を行う．同じバイオメトリクスであり行動的特徴に該当するキーストローク認証と類似しているが，キーとなるボタンが存在せず，キャンバス上の任意の位置をタップすることができる点で異なる．表 1 にリズム認証の利点と欠点を示す．

表 1　リズム認証の利点と欠点

Table 1　Advantages and disadvantages of the rhythm authentication.

利点	欠点
ボタンレスなので入力情報が読み取られにくい	リズムを再現できなければ認証されない
認証は画面タップのみで煩わしさが少ない	
特別な機器が不要であり導入コストが安価	

3. リズム認証実験

3.1 実験目的

本研究におけるリズム認証では，利用者がリズムを作成し，登録を行い，登録されたデータをもとに認証が行われる．先行研究では，被験者がリズムを一から考え，リズム作成を行っている．しかし，それではリズムが単調なものに偏る可能性があることや，時間の経過により，リズムを再現することが困難になるなどの問題がある．本実験では，指定楽曲の主旋律を用いリズム作成をした際，先行研究に比べ認証精度が向上することを目的とする．

3.2 実験方法

被験者として，本学学生 10 名に協力してもらった．先行研究において音楽経験年数が 3 年以下のもののみを対象としている．図 1 に示すように被験者は椅子に座った状態でスマートフォンを片手で持ち，持った手の親指で画面をタップする．

まず，被験者には，指定楽曲（long）として，神奈川工科大学校歌の一部（4 小節 1 拍）を切り取った曲を聴いてもらう．その後，指定楽曲（long）を用い，4 タップで一試行として画面をタップするリズムを考えてもらった．実機での練習後，被験者がリズム定着したと感じたタイミングで，登録，認証用として入力を 5 回行う．その後，切り取った曲をさらに縮めた（2 小節 1 拍）指定楽曲（short）を用い，同様に実験を行った．図 2 に実験の流れを示す．

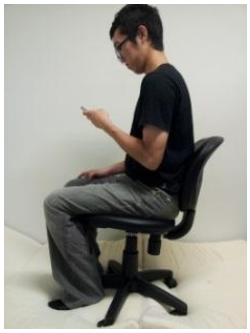

図 1　実験の様子

Figure 1　Experiment image.

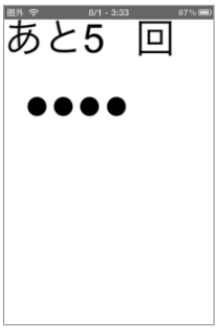

図 3　実験プログラム

Figure 3　Measuring software.

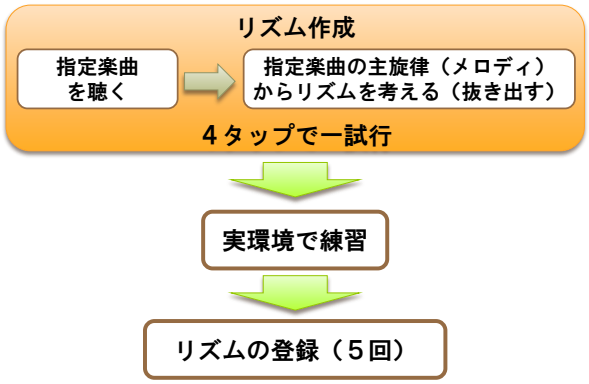

図 2　実験の流れ

Figure 2　Experimental procedure.

3.3 実験環境

実験で使用した機器を表 2 に示す．

表 2 実験に使用したスマートフォン

Table 2　Labware.

機器名	iPhone4
OS	iOS5.1.1
タッチパネルサイズ	3.5 インチワイド

3.4 実験プログラム

実験プログラムは HTML5 の Canvas を使用して作成した．図 3 に示すように，画面には残りの試行回数が表示されており，一試行ごとに回数表示が減る仕組みになっている．

また，画面を押下することで赤色の丸印が点灯し，解放することで緑色の丸印が点灯するようになっている．画面全体に Canvas を広げており，画面上にあるどの位置をタップした場合でも 1 回としてカウントされる．

3.5 分析方法

本研究では，SOM を用いることにより本人特定を行う．各被験者の登録用の計測データからマップを作成し，作成されたマップに認証用データを投入する．

5 回分の計測データを最大値 1，最小値 0 に正規化したものを登録用に 4 回分，認証用に 1 回分と分け，SOM による学習で得た座標結果から，ユークリッド距離を算出し，分析にはそれらの平均ユークリッド距離を用いた．また，SOM の学習条件は，マップサイズ 50×50（ユニット数 2,500），学習回数 50,000 回と設定している．

3.6 分析に用いた属性ベクトル

画面タップのパターンを計測し，SOM 学習用の属性ベクトルを構成し，分析に用いた．画面タップ時の画面押下から，その直後のイベントとの時間差 t1～t7 をそれぞれ計測し，分析に用いている．計測属性を図 4 に示す．

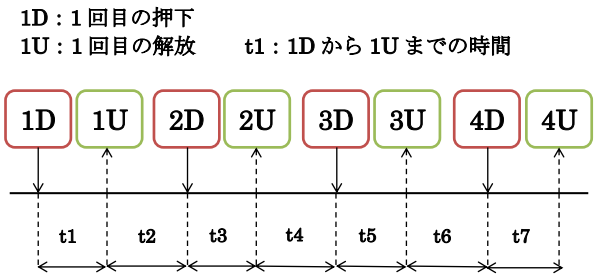

図 4　分析に用いた属性ベクトル

Figure 4　Attribute vector.

3.7 評価方法

本人拒否率（FRR：False Reject Rate）と，他人受容率（FAR：False Accept Rate），これらの分布グラフ交点にあたるエラー率，等価エラー率（EER：Equal Error Rate）の値を 1 から引いた値を認証精度としている．

4. 実験結果

指定楽曲（long）で得られた認証精度結果を表 3 に，指定楽曲（short）で得られた認証精度結果を表 4 に示す．SOM の初期値は乱数で決まる特徴があり，毎回異なるマップが生成される．そのため，指定楽曲（long），指定楽曲（short）それぞれマップを 10 回分作成し，それらの平均を本実験における認証精度とした．

指定楽曲（long）において認証精度に最も近い SOM 作成 10 回目の認証精度グラフを図 5，指定楽曲（short）において認証精度に最も近い SOM 作成 10 回目の認証精度グラフを図 6 に示す．また，SOM マップを図 7，図 8 に示す．

表 3　認証精度結果（指定楽曲 long）

Table 3　Authentication accuracy(long version）.

SOM 作成回数	閾値	FRR [%]	FAR [%]	認証精度 [%]
1 回目	13.0-13.5	10.0	10.0	90.0
2 回目	9,0-9.5	3.0	3.0	97.0
3 回目	8.5-9.0	3.0	3.0	97.0
4 回目	9,0-9.5	3.0	3.0	97.0
5 回目	12.0-12.5	6.0	6.0	94.0
6 回目	8.0-8.5	3.0	3.0	97.0
7 回目	9,0-9.5	2.0	2.0	98.0
8 回目	9.5-10.0	2.0	2.0	98.0
9 回目	10.0-10.5	3.0	3.0	97.0
10 回目	10.0-10.5	3.0	3.0	97.0
認証精度				96.2

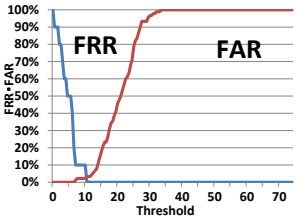

図 5　認証精度グラフ（指定楽曲 long）

Figure 5　Authentication accuracy(long version）.

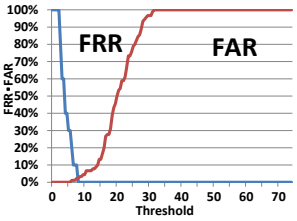

図 6　認証精度グラフ（指定楽曲 short）

Figure 6　Authentication accuracy(short version).

表 4　認証精度結果（指定楽曲 short）

Table 4　Authentication accuracy(short version).

SOM 作成回数	閾値	FRR [%]	FAR [%]	認証精度 [%]
1 回目	7.5-8.0	4.0	4.0	96.0
2 回目	6.0-6.5	1.0	1.0	99.0
3 回目	6.5-7.0	1.0	1.0	99.0
4 回目	8.5-9.0	3.0	3.0	97.0
5 回目	6.5-7.0	1.0	1.0	99.0
6 回目	6.5-7.0	1.0	1.0	99.0
7 回目	6.5-7.0	1.0	1.0	99.0
8 回目	6.5-7.0	1.0	1.0	99.0
9 回目	7.5-8.0	2.0	2.0	98.0
10 回目	7.5-8.0	2.0	2.0	98.0
認証精度				98.3

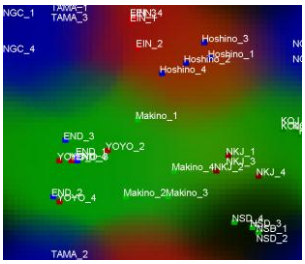

図 7　SOM マップ
（指定楽曲 long）
Figure 7　SOM map
(long version）.

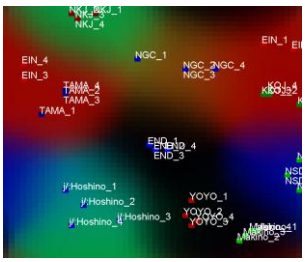

図 8　SOM マップ
（指定楽曲 short）
Figure 8　SOM map
(short version).

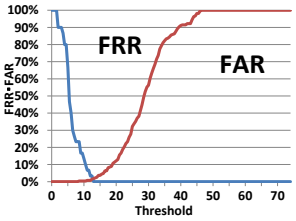

図 9　認証精度グラフ
（音楽経験年数 6 年以上）
Figure 9　Authentication accuracy(over 6 years musical experience).

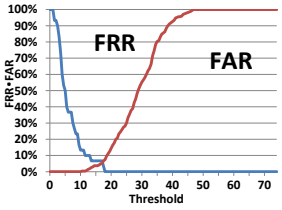

図 10　認証精度グラフ
（音楽経験年数 3 年以下）
Figure 10　Authentication accuracy(less than 4 years of musical experience).

5.　考察

指定楽曲（long）では認証精度 96.2%，指定楽曲（short）では認証精度 98.3%という結果を得た．図 9，図 10 に先行研究で行ったリズム認証実験，音楽経験年数でグループ分けした際の認証精度グラフを示す. 図 10 のグラフと本実験の図 5，図 6 のグラフを比較すると，本実験のグラフはどちらも FRR の値が優れていることがわかる．また，本実験における被験者は，音楽経験年数が 3 年以下のもののみを対象としているため，図 9 の音楽経験年数が 6 年以上のグループと比較するとやや認証精度は劣るが，FRR に関しては図 9 よりも優秀な値を示している．このことから，指定楽曲（楽曲の主旋律）を用いたことで，リズムの再現性が向上したといえる．

指定楽曲 (short)，指定楽曲 (long) では，指定楽曲 (long) がリズム選択の幅が広く，FAR が優れた値になると予想していたが，図 5，図 6 を比較すると同程度となっている．図 6 に示している SOM マップで，2 名の被験者が非常に近い座標にクラスタリングされているのがわかる．近い座標にクラスタリングされているということは，一方の被験者が認証を試みた際に，もう一方の近い座標に位置している被験者と誤認識してしまう可能性が高いことを示す．このことから．2 名が似通った特徴のリズムを登録しており，結果的にリズムの選択幅が広い指定楽曲（long）と選択幅が半分の指定楽曲（short）において FAR が同程度となったと考える．

指定楽曲（short）が指定楽曲（long）と比較して FRR が優れているが，本実験の流れは，図 2 に示すとおり，曲を覚えてからリズム作成という流れのため，4 小節程度では負担が大きく，2 小節程度に設定するのがよいという可能性をあらわしている．しかし，指定楽曲（long）の後に指定楽曲（short）の検証実験を行ったため，被験者が慣れたという可能性も考えられる．この点については，より詳細な検証が必要である．

6.　おわりに

本研究は，スマートフォンにおいて画面をタップする際の個人の特徴をもとに本人識別を行い，利便性，安全性を兼ねた有用なセキュリティ向上策としてリズム認証の提案を行っている．

本実験では，スマートフォンにおけるリズム認証手法において，音楽経験年数 3 年以下を対象として，指定した楽曲の主旋律を用いリズム作成を行った際のリズム特徴量を抽出し認証精度を求めた．結果，指定楽曲を用いた際，FRR が先行研究に比べ優れた値を示し，認証精度が指定楽曲（long）の際 96.2%，指定楽曲（short）の際 98.3%と先行研究に比べ高い結果となった．さらに精度を向上させるためには，リズム登録の際に，一定の閾値を超えた値をエラーデータとし，エラーデータを取り込めないようにプログラムで管理することが有効だと考える．今後は，本手法が先行研究に比べ利用者への負担はどの程度なのか検証を行っていき，より利用者が負担だと感じない仕組みを考える必要がある．また，時間経過した場合に本手法がどの程度リズムを再現することができるか検証を行っていきたい．

参考文献

1)　市村亮太，野口敦弘，納富一宏，斎藤恵一:"スマートフォンにおける覗き見攻撃耐性を考慮した個人認証方式の提案"，ヒューマンインタフェース学会 ヒューマンインタフェースシンポジウム 2012, 3431S, pp.1065-1066, (2012).
2)　市村亮太，野口敦弘，納富一宏，斎藤恵一:スマートフォンにおけるリズム認証手法の検討，電子情報通信学会 2012 年度 HCG シンポジウム II-4-2，pp.222-225，(2012).
3)　市村亮太，野口敦弘，納富一宏，斎藤恵一:"自己組織化マップを用いたスマートフォンにおけるリズム認証手法"，バイオメディカル・ファジィ・システム学会 第 25 回年次大会講演論文集，pp.27-30, (2012.12).
4)　大北正昭，徳高平蔵，藤村喜久郎，権田英功：自己組織化マップとそのツール，p.1，pp.1-7，加藤文明社，2008.
5)　バイオメトリクスセキュリティコンソーシアム：バイオメトリックセキュリティ・ハンドブック，p.2，pp.15-18，p3，pp.1-2，オーム社，2005.
6)　野口敦弘，納富一宏，斎藤恵一:"ボタンレスで行うリズム認証手法～ピアノ経験者との比較によるリズムの個人差検証～"，情報処理学会 マルチメディア，分散，協調とモバイル（DICOMO2012）シンポジウム，1F-3, pp.192-196, (2012).